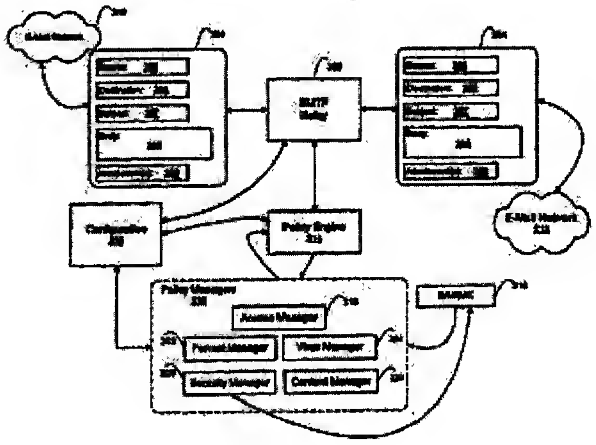
E-MAIL FIREWALL WITH STORED KEY ENCRYPTION/DECRYPTION

Publication number: JP2001518724 (T)
Publication date: 2001-10-16
Inventor(s):
Applicant(s):
Classification:
- international: ***G06F13/00; G06F1/00; G06F21/00; H04L9/00; H04L9/14; H04L12/22; H04L12/58; H04L29/06;*** **G06F13/00; G06F1/00; G06F21/00; H04L9/00; H04L9/14; H04L12/22; H04L12/58; H04L29/06;** (IPC1-7): H04L12/66; G06F13/00; H04L9/14; H04L12/22; H04L12/54; H04L12/58
- European: H04L29/06S2B; H04L12/58F; H04L29/06S2B2; H04L29/06S4B
Application number: JP20000504677T 19980723
Priority number(s): US19970053668P 19970724; WO1998US15552 19980723

Also published as:
- JP3932319 (B2)
- WO9905814 (A2)
- WO9905814 (A3)
- US2007214353 (A1)
- US7380274 (B2)

more >>

Abstract not available for JP 2001518724 (T)
Abstract of corresponding document: **WO 9905814 (A2)**



An e-mail firewall (105) applies policies to e-mail messages (204) between a first site and a plurality of second sites in accordance with a plurality of administrator selectable policies (216). The firewall comprises a simple mail transfer protocol (SMTP) relay (202) for causing the e-mail messages (204) to be transmitted between the first site and selected ones of the second sites. A plurality of policy managers (216) enforce administrator selectable policies. The policies, such as encryption and decryption policies, comprise at least a first source/destination policy (218), at least a first content policy (220) and at least a first virus policy (224).; The policies are characterized by a plurality of administrator selectable criteria (310), a plurality of administrator selectable exceptions (312) to the criteria and a plurality of administrator selectable actions (314, 316, 322) associated with the criteria and exceptions. The policy managers comprise an access manager (218) for restricting transmission of e-mail messages (204) between the first site and the second sites in accordance with the source/destination policy (218). The policy managers (216) further comprise a content manager (220) for restricting transmission of e-mail messages (204) between the first site and the second sites in accordance with the content policy (220), and a virus manager (224) for restriction transmission of e-mail messages (204) between the first site and the second sites in accordance with the virus policy (224).

Data supplied from the ***esp@cenet*** database — Worldwide

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]
Especially this invention relates to the security for an electronic mail system, concerning the computer security field generally.
[0002]
[Description of the Prior Art]
The new way for operating level communication and electronic commerce technology (EC) was cut by the E-mail (E-Mail) accompanying growth and omnipresence of the Internet, and the extensive use of groupware. An organization comes to be dependent on E-Mail which passed the Internet for transmission of important files, such as a purchase order in an in-house, a sales forecast, financial information, and a contract, gradually, and has come to be dependent on E-Mail gradually also among different organizations for the same processing. In such a situation, those files serve as important property which must be protected.
[0003]
In order to guarantee the present-day confidentiality and integrity of data communications, many security references exist conventionally. For example, the conventional firewall prevents network access by a user without authority. Secure socket art (Secure Socket Technology) makes it possible to send data safely via World Wide Web (WWW). However, a problem still has much E-Mail which is the use on the Internet projected most in respect of security for almost all organizations. Many conventional firewalls restrict access to the information only protected by this firewall.
It does not have the capability to restrict transmission of the information on the outside of the in-house by E-Mail.
This passes to the viral infection by accidental or intentional disclosure of the extra sensitive

information by E-Mail being emitted from an in-house, and E-Mail included in an in-house.

[0004]

Encryption of this message is mentioned as one method for protecting airtightness or an E-Mail message. Security can be obtained by the digital signature which provides attestation of an E-Mail message. Each of encryption and attestation is supported with the S/MIME (Secure/Multipurpose Internet Mail Extensions) messaging protocol. This protocol, By IETF (International Engineering Task Force). The document it is ["S/MIME Message Specification" (1997) and "S/MIME Certificate Handling" (1997) which were published] entitled is specified. Each user can carry out encryption / decryption, and attestation of an E-Mail message using commercial software. However, implementation of this work that uses software will not restrict with an always simple thing, but, so, the ease of original use of E-Mail as a means of communication may be spoiled. The organization which desires to use this software has to leave encryption of all the needed messages to each user, without having a means for performing CC in any way. In addition, many conventional firewalls do not have the capability to control the contents or form of a fixed message of frequenting an organization. For example, many conventional firewalls do not have the capability to guarantee that E-Mail is meeting the fixed standards, like contents or sauce and/or the destination address, or the domain is enciphered. Many conventional firewalls do not have the capability to control the message which is not desirable as for the E-Mail advertisement included in an in-house etc. which are not welcomed.

[0005]

[Problem(s) to be Solved by the Invention]

Therefore, the E-Mail firewall which provides the improved CC to the E-Mail message which goes in and out to an organization is needed.

[0006]

[Means for Solving the Problem]

In a main mode, this invention provides an E-Mail firewall (105) which sifts out an E-Mail message (204) which occurs within a computer network (101,103) or enters into the network. An embodiment which adopted a principle of this invention takes advantageously a form of an E-Mail control system (105) which controls an E-Mail message (204) transmitted and received between computing sites. This E-Mail control system (105) is provided with a message encoding means (526) which enciphers a message (204) of a type with which the 1st transmitted from a computing site was specified according to an encryption key (528) with which the at least 1st was stored. A code of a message (204) of a type with which the 2nd by which a message decryption means (552) was received by computing site according to an encryption key (528) with which the at least 2nd was stored was specified

It decodes. A filter (216) supervises a message (204) according to filter information (216) which can be changed before encryption after decryption by said message decryption means (552), and by said message encoding means (526).

[0007]

There is an important advantage of this embodiment in CC of an E-Mail policy by an organization increasing. All the E-Mail messages generated in entering or an in-house can be enciphered or deciphered according to a policy on which it was imposed by organization to an in-house, and it can filter. For this reason, each user of a desktop computer of an in-house does not need to be concerned with following an E-Mail policy of this organization certainly. An E-Mail message can be supervised about sauce or a destination specific about specific contents.

[0008]

An embodiment which adopted a principle of this invention also advantageously acts as a transparent existence to each user of an in-house. For example, each user of this does not need to be concerned with following an encryption policy of an organization. It can encipher automatically and/or an E-Mail message which is emitted from an E-Mail message including specific contents, a specified address, or a domain, or is transmitted to this address or a domain can be filtered. For example, other organizations (for example, the company B) and an organization (for example, the company A) which exchanges E-Mails frequently, When it is judged that all the E-Mails to the company B should be enciphered on security, it is possible to build an E-Mail firewall in the above companies A, and to recognize a domain name of the company B, and to store an encryption key. It will be enciphered by above-mentioned E-Mail firewall, without all the E-Mail messages to the company B needing additional operation by each user from the company A after that. When the company B has already built an E-Mail firewall which adopted an above-mentioned principle, this E-Mail firewall can be built so that a message from the company A may be deciphered. Therefore, each addressee in the company B which received E-Mail from the company A does not need to perform additional operation, in order to decipher E-Mail from the company A. Therefore, all the E-Mail messages to the company B become possible [exchanging without an intervention by a user certainly also in the company A or the company B] from the company A. Of course, an E-Mail firewall of the company B can be constituted so that same E-Mail message transmission to the company A may become possible from the company B.

[0009]

It is possible to carry out another policy to message transmission between the companies A and B. For example, by constituting using a rule which recognizes an E-Mail message which contains a specific term or a phrase for an above-mentioned filter of the target E-Mail firewall, and prevents the transmission, It is possible to reduce accidental (or it is intentional) disclosure of specific information between the companies A and B. An E-Mail firewall can also be constituted again so that an exception over this rule may be used. For example, it is possible to carry out E-Mail from a specific user or E-Mail to a specific user outside of an object of application of this rule. After transmission of a message is prevented, operation performed by E-Mail firewall can be changed. For example, it is possible to return a message which poses a problem to a sending person with an explanation message. In order that an administrator may see alternatively in addition to the above, it is possible to store the message concerned or to delete this message. (It relates to one, or two domains or each addresses or more, respectively) Many encryption keys can be stored in an E-Mail firewall which adopted an above-mentioned principle, and many domains and/or safe communication with each user can be enabled.

[0010]

**** and other advantages of this invention will be further understood by fitness by referring to the following detailed explanation.

[0011]

[Embodiment of the Invention]

In drawing 1, the E-Mail network 101,102 is connected to the E-Mail network 103 via WAN (Wide Area Network) 104, such as the Internet. Between the Internet 104 and the E-Mail network 101,103, the access firewall 106 and the E-Mail firewall 105 are allocated. The E-Mail network 102 is connected to the Internet 104 by only the access firewall 106. The E-Mail network 101,102,103 takes the conventional gestalt, respectively. For example, the E-Mail networks 101-103 can take the form of two or more LAN which supports one LAN (Local Area Network), one, or two conventional E-Mail messaging protocols or more. The access firewall 106 can also take the conventional gestalt. The access firewall 106 operates so that access to the file from the machine arranged in the remote place stored in the computer network (the E-Mail network 101 - 103 grades) may be restricted. The E-Mail firewall 105 (the numerals 105.1 and 105.2 show separately) can take advantageously the form where it explains in detail in this book, in order to control transmission of the E-Mail message between one internal site, one, or two external sites or more. For example, one internal site about the E-Mail firewall 105.2 can take the form of the E-Mail network 103. The external sites about the E-Mail firewall 105.2 are all sites that are not included in the E-Mail network 103. For example, the external sites about the E-Mail firewall 105.2 are the arbitrary sites in the E-Mail network 101,102, and all sites of the others connected to the Internet 104. The E-Mail firewall 105 is arranged suitably at the access firewall 106 "safe side." Drawing 1 should be understood as what shows the principle of the embodiment written in this book, for example. The access firewall 106 is not required for operation of the embodiment which was shown for the purpose of illustrating this invention and adopted the principle of this invention.

[0012]

Suitably, the E-Mail firewall 105 takes the form of the program executed on the conventional general purpose computer. Windows NT available [with a typical embodiment] from Microsoft Corporation (Redmond, Washington) in a computer An operating system (trademark) is performed. Although the E-Mail firewall 105 is shown by drawing 1 as what operates about an E-Mail message between an internal site and an external site, It is also possible to use this E-Mail firewall 105 and to exchange messages between two internal sites of two or more computer networks which have the messaging backbone according to SMTP.

[0013]

The block type showing the main functional components of the E-Mail firewall 105.1,105.2 shows drawing 2. In the figure, the SMTP (Simple Mail Transfer Protocol) relay module 202 achieves the conventional Internet relay host's function. The Internet relay host's example is a sendmail program. The SMTP relay module 202 transmits and receives an E-Mail message (the numerals 204 show) between the internal site 210 and the external site 212. The E-Mail message 204, The E-Mail address of the sauce of this message 204. The destination field 206 which specifies one or two destination E-Mail addresses or more, the source field 205 and this message 204, to specify, the subject field 207 which specifies the title (namely, subject) of this message 204, . Called it the attachment field 209 which specifies one or two files or more which should transmit with the field 208 of a main part which specifies the main part (a text and/or graphics data are included) of this message 204, and this message 204. The form of the conventional E-Mail message including two or more user appointed information fields is taken. Although the priority of a message, a transmitting side agent's identifier, and the time of a message are mentioned as the other user appointed fields, the user appointed field is not limited to these.

[0014]

The E-Mail message 204 can be encoded according to one of two or more encoding forms which are explained in full detail below. As for the SMTP relay module 202, it is preferred to take the form of the conventional software module which transmits and receives an E-Mail message according to the SMTP protocol specified by Internet RFC821. An SMTP protocol is not important for this invention, and in other examples. It is possible to transpose an SMTP relay module to the module which transmits and receives a message in another forms, such as FTP (File Transfer Protocol) or HTTP (Hyper-Text Transfer Protocol).

[0015]

As for the SMTP relay module 202, it is preferred to be constituted so that it may opt for routing to the addressee of a message using DNS (Domain Name System), It is possible to relay a message to the SMTP host specified by the administrator alternatively. When DNS is chosen, the default SMTP host can still specify, in order to enable transmission of a message, even if it is a case where DNS service cannot be used. The routing option can carry out an override per domain. The SMTP relay module 202 makes it possible to make it possible going up between also advantageously specific hosts, or to get down and to restrict SMTP connection of a direction for things, and to refuse connection between specific SMTP hosts.

[0016]

Drawing 3 shows the mode in which the message from the internal site 210 and the external site 212 received with the SMTP relay module 202 is processed by the policy engine 214. The policy engine 214 receives the message from the SMTP relay module 202, It judges which policy is applicable to this message by creating the list 302 of sending person policies about the sending person (sauce) 205 of this message, and creating the list 304,306,308 of addressee policies for every addressee. Subsequently, the policy engine 214 calls the policy manager 216, in order to apply each policy. The policy of a different type has a predetermined priority about the application. For example, a code release policy is applied before other policies, and it enables the policy which acts about the field 208 of a main part of a message to access by this the contents included in this main part. At an alternative embodiment, the turn that a policy is applied can be chosen by a system administrator. An access manager policy is applied after a decryption policy, and, subsequently other policy managers are repeatedly called in the turn suggested by the policy which should be applied to a message. Subsequently, the policy engine 214 receives the result from a policy manager, and transmits a message to the SMTP relay module 202 according to the this received result. The result received with this policy engine 214 comprises actions explained in full detail in this book, such as treatment, notes, and a notice. The processing result of the message 204 with the policy engine 214 generates two or more additional messages (for example, notice to a sending person, an addressee, or a system administrator). According to a suitable embodiment, the policy engine 214 is carried out as a program executed with a digital computer.

[0017]

The policy manager 216 can operate so that forcible execution of the policy inputted by the administrator of the E-Mail firewall 105 may be carried out. As for the policy manager 216, it is preferred to comprise two or more modules for carrying out forcible execution of the policy constituted by the administrator for the E-Mail message of a specific form. For example, in the E-Mail firewall 105 the policy manager 216, Two or more manager modules including the access manager 218, the contents manager 220, the format manager 222, the virus manager 224, and the security manager 226 are carried out. As for the policy manager 216, it is preferred to be developed by the input inputted by the administrator via the composition module 230. According to the information inputted by the administrator, the composition module 230 operates again so that the SMTP relay module 202 and the policy engine 214 may be constituted. The policy manager who shows drawing 2 and explains here used to aim only at illustration of a model embodiment. It also has intention of the policy manager of other types as a thing in a principle given in this book.

[0018]

The access manager 218 provides compulsive execution of access control policies, such as a destination to which transmission of E-Mail was forbidden, or sauce which cannot receive E-Mail. The access manager 218 can filter the message exceeding the maximum message size determined by the administrator again, or the message which includes a specific word all over the subject field 207. The access manager 218 can also filter a message with the priority of the message specified by the user. For example, while sending the message of a high priority promptly so that drawing 7 may be explained in full detail below, it is possible to put the message of a low priority into queuing. The access manager 218 can filter a message by the transmission date and/or time of a message again. For example, the message transmitted to the specific time zone of the one day or the specific day (for example, a weekend or a holiday) can carry out the maintenance or further filtering (for example, contents manager 220).

[0019]

The contents manager 220 supports compulsive execution of a contents control policy. Suitably The word in the field 208 of (a) main part with the specific contents manager 220, (b) Support filtering by 1 of the standards of the specific word in the subject field 207 or the field 208 of a main part, and (c) attachment field 209 (the all, or a name/type), or two or more. A contents control policy and other suitable policies can be specified that it needs a specific material (for example, a specific notice or refusal). The virus manager 224 supports compulsive execution of a virus control policy by detecting the E-Mail attached file infected with the virus. As for the virus manager 224, it is preferred to detect the virus contained in the compressed file format of the plurality containing PKZip, PKLite, ARJ, LZExe, LHA, and MSCompress. For example, the virus manager 224 can use a commercial virus scan engine. As for the virus manager 224, it is preferred to apply a policy again to "a clean message, i.e., the message the virus scan being carried out and not being infected with a virus turns out to be." The "clean stamp" notes which show that a virus was not detected are given to this message.

[0020]

The format manager 222 provides conversion of the E-Mail message to the 1st format [2nd] from a format. According to a suitable embodiment, the format manager 222 changes a message into a MIME format from a UUENCODE format. Suitably, the format manager 222 changes a message in advance of the message processing by other policy managers.

[0021]

As for the security manager 226, it is preferred to carry out forcible execution of two or more E-Mail encryption policies. Suitably, the security manager 226 does forcible execution of a client security use policy, a code protection policy, a plain text access policy, and the default action policy. The security manager 226 applies again the proxy encryption and the signature policy which are explained in full detail below in relation to drawing 5 (b) instead of a user.

[0022]

A client security use policy specifies what a specific user should perform encryption or a signature for by a desktop. In order to show the time when forcible execution of this policy should be carried out, it is possible to set up an additional standard. For example, it is possible to specify E-Mail to the lawyer of a company from CEO of the company by the domain or a full E-Mail address as what needs encryption or a signature, and to carry out forcible execution of the representative-client privilege, and to suspend an encryption policy. What the message which uses a client security use policy, is already in encryption form, and probably meets other standards should be saved for (if it puts in another way) It is possible to specify what processing by the E-Mail firewall 105, correction, or decryption is not performed for. A plain text access policy needs to design the E-Mail firewall 105 as an addressee of a message by whom the specific type was specified. The E-Mail firewall 105 is specified as an addressee of an encryption message, in order to apply access, contents, a virus, and other policies to a message. A plain text access policy can be used in order to send the notice with a signature to the sending person of a message again as one method of providing the sending person of a message with the public key of the E-Mail firewall 105. A default action policy is a message which is not enciphered, and it shows action which should be performed about the optional message which meets other standards of a certain selectively, without being enciphered by the E-Mail firewall 105. This policy type is used in order to ensure that a specific message is enciphered by somewhere (a desktop or E-Mail firewall 105).

[0023]

As for a policy, it is preferred to be inputted by the permitted administrator via the composition module 230, and, as for this composition module 230, it is preferred to take the form of the program executed on the computer by which the program was stored. A policy can be individually applied advantageously by the group of an E-Mail domain or others to a user. Drawing 4 shows the mode to which a policy is applied. The user can compose of hierarchy-like directory structure so that the grouping of a user and/or a domain may become easy. When a policy is applied to a given directory, the policy which requires the subdirectory corresponding to a directory given [this] is inherited. For example, in drawing 4, the policy 1 is applied to the subdirectory 404 and applied to all the subdirectories, a domain, and a user (for example, the subdirectory 412, the user 408, and the domain 410) by extension. This is performed unless the override of this policy is clearly carried out by another policy applied to the specific subdirectory or the intervening subdirectory. For example, about the user 1 (the numerals 408 show), the policy 3 carries out the override of the policy 1, when competition exists between this policy 3 and the policy 1, and when competition does not exist, it will compensate the policy 1. The exception 1 will carry out the override of the policies 1 and 3 about the specific exception specified with the exception 1. As shown in drawing 4, the policy 1 is applied to the user 414,416,418, when competition exists, the override of it is carried out by the policy 2 about the user 414,416,418, and when competition does not exist, it will supplement. Thereby, it becomes also advantageously possible to apply a policy to an user group easily. However, the exact mode in which a policy is stored is not important for this invention, and it is possible to adopt various storing means and storing form.

[0024]

The E-Mail message 204 which was received by the SMTP relay module 202 and/or was transmitted, By IETF (Internet Engineering Task Force). S/MIME (Secure/Multipurpose.) specified in the document it is ["S/MIME Message Specification" (1997) and "S/MIME Certificate Handling" (1997)] entitled It is preferred to be encoded according to an Internet Mail Extension protocol. To an advantageous thing, this S/MIME protocol, Security is built by the top layer of an engineering specification MIME protocol according to RSA Data Security and Public Key Cryptography Standards (PKCS: public-key-encryption-ized standard) specified by Inc. Also advantageously, S/MIME provides the security service about the privacy using the attestation and encryption which used the digital certificate. A digital certificate, Also as "the ITU-T recommendation X.509" (June, 1997). "It is known Information Technology. - It is preferred to carry out according to the X.509 format specified by Open Systems Interconnection - The Directory:Authentication Framework." As for encryption, it is preferred that one of symmetrical encryption algorithm DES, Triple-DES, and RC2 performs. It is a well-known thing, and the S/MIME protocol is used widely, provides encryption and a digital signature, and is [therefore] preferred as a communications protocol. However, the details of operation of this protocol are not important for this invention. It will be understood that it is also possible to use other safe messaging protocols called PGP (Pretty Good Privacy) or OpenPGP specified by the ITF workgroup.

[0025]

The access manager 218 is a policy manager of the beginning for processing the E-Mail message 204. The access manager 218 acts only about the message header information which is not enciphered. For this reason, the access manager 218 processes the E-Mail message 204 in advance of decryption with the S/MIME engine 215. Generally the term "message header information" points out the portion except the field 208 (generally called a message text) of a main part, and the attachment field 209 among messages. Therefore, header information includes a source field, the destination field, and a subject field (205,206,207). As other fields which can be contained in a message header, a date / time stamp, a priority, and a transmitting side agent are mentioned. The remaining modules act on the message 204 after processing with the S/MIME engine 215. As for the format manager

222, like previous statement, it is preferred to act on a message in advance of the operation by other managers, such as the virus manager 224, the security manager 226, and the contents manager 220.

[0026]

An S/MIME protocol makes it possible to exchange the E-Mail message 204 with two safe sites which support an S/MIME protocol. When a transmitting site and a receiving site perform an S/MIME function, a virtual private network (VPN) as shown in drawing 5 (a) can be attained. VPN (here, "object level E-MailVPN" is called) obtained as a result provides encryption / signature of the message between a transmitting site and a receiving site, and/or decryption/verification. In object level E-MailVPN shown in drawing 5 (a), it is enciphered separately and each object (message) is sent via a standard (SMTP) transmission medium. In this case, each object is deciphered by the other end. This object level E-MailVPN does not need the safe real-time connection needed by the conventional VPN for an advantageous thing. As shown in drawing 5 (a), the mail server 105.1,105.2 performs the function explained in this book about the E-Mail firewall 105, and object level E-MailVPN is attained among them as the result. E-Mail enciphered and transmitted with 105.1,105.mail server 2 admiration, After passing the server with huge E-Mail transmitted via the Internet 104 which is not safe, in spite of the fact of reaching the destination (namely, address), it is protected from the indication to a third party. In this exchange, the E-Mail firewall 105.1,105.2 provides generation of the key of a couple, and a key certificate, and provides exchange of the public key certification in automatic or hand control with other S/MIME servers. In addition, the E-Mail firewall 105.1,105.2 enables selection of discernment of other S/MIME servers through a directory domain record, the combination of a directory domain record with a server certificate, encryption/signature algorithm, and key length. The directory domain record and the directory user record explained below are indicated to drawing 4.

[0027]

Exchange of the message encoded [S/MIME] can also be performed again between the E-Mail firewall 105.1,105.2 and the S/MIME client connected to the server which does not perform an S/MIME function. Drawing 5 (b) shows the data exchange between the S/MIME clients connected to the E-Mail firewall 105 and the non-S/MIME server 506. In drawing 5 (b), the server 105.1 performs encryption and decryption of a message instead of the client 502, and, generally provides the above-mentioned function about the E-Mail firewall 105.1,105.2. In detail, in this exchange, the E-Mail firewall 105.1 provides generation of the key of a couple, and a public key certification, and provides exchange of the public key certification in automatic or hand control with the client 508.1. In addition, the E-Mail firewall 105.1 enables selection of discernment of the client 508.1 through a directory user record, the combination of a directory user record with an user certificate, encryption/signature algorithm, and key length. The client

508.1 provides encryption/decryption service, in order to make it possible to transmit a message safely via the server 506 by supporting encryption/decryption service. In drawing 5 (b), object level VPN (here, "proxy security" is called) specific type is attained between the server 105.1 and the client 508.1. In proxy security, at least one client (client 508.1 grade in drawing 5 (b)) is concerned with execution of encryption/decryption. The encryption/code in which this is performed by the server 105.1,105.2

It is contrastive with the composition of drawing 5 (a) where decipherment service is not in sight from the client 502.1,502.2.

[0028]

In drawing 5 (a), although the communication between the servers 105.1,105.2 is safe, the communication between the client 502.1,502.2 and each server 105.1,105.2 is not safe. In the equipment which many require, security is unnecessary. However, when this security is desired, it is possible to mount encryption/decryption service also in the client 508.1,508.2, and to perform proxy security. The server 105.1,105.2 in drawing 5 (c) performs the same function as what was mentioned above about drawing 5 (a), therefore attains object level VPN. In addition, the client 508.2,508.1 enables safe communication between the corresponding servers 105.1,105.2. The encryption/decryption performed by the server 105.1,105.2 should care about that it is possible to have become independent of the encryption performed by the corresponding client 508.2,508.1. For example, the message from the client 508.2 to the client 508.1, It is enciphered at the time of transmission to the server 105.1, and is deciphered by the server 105.1, Receive suitable action by a policy manager and, subsequently to [for transmission to the server 105.2], it is enciphered, This client 508.1 is able to be deciphered by the server 105.2, to receive suitable action by a policy manager, to be enciphered subsequently to [for transmission to the client 508.1], and to decipher a message.

Alternatively the message from the client 508.2 to the client 508.1, It is enciphered by the client 508.2 and suitable action to non-enciphering portions (destination field etc.) is received, Subsequently, it is again enciphered by the server 105.1 for the transmission to the server 105.2 of the whole (the portion which is not enciphered by the client 508.2 is included) message, In order that this server 105.2 may decode encryption by the server 105.1 and may decode the encryption performed by the client 508.2, it is possible to transmit a message to the client 508.1. The combination of the two above-mentioned scenarios is also feasible.

[0029]

Each E-Mail message 204 processed by the E-Mail firewall 105 is processed according to the step shown in drawing 6 (a) and drawing 6 (b). Drawing 6 (a) is a flow chart which shows operation of the E-Mail firewall 105 according to the message which received. Drawing 6 (b) is a flow chart which shows operation of the E-Mail firewall 105 before transmitting a message. The message processed by the E-Mail firewall 105 may receive from an external site, in order to receive from an internal site in order to receive from an internal site in order to transmit to an internal site, or to transmit to an external site, or to transmit to an internal site. All single messages can include an inside and the external destination 206. The step shown in drawing 6 (a) and drawing 6 (b) is performed by generating the sending person policy and addressee policy which are shown in drawing 3. therefore, for every each of two or more destinations, the step shown in drawing 6 (b) can be performed variously, and it has a different result for every different destination.

[0030]

Drawing 6 (a) is referred to here. At Step 602, it is judged whether decryption of the portion of the message 204 is required for the E-Mail firewall 105. When decryption is required, according to the key 628 stored, decryption is performed at Step 604. After this decryption when decryption is unnecessary, The E-Mail firewall 105 applies the policy manager 216, and this policy manager 216 performs action (Step 610,612,614,616 shows) of four types to the E-Mail message 204. The standard action 610 provides a filtering reference with the selected administrator. The exception action 612 judges which standard 610 is excepted. It will be possible to choose two or more standards 610, and the logic AND operation of a standard will arise as a result. It will be possible to choose two or more exceptions 612, and an exceptional logic OR operation will arise as a result. That is, the trigger of the policy will be carried out to any one of exception conditions being truth. The notes action 614 produces generation of the attachment field to the message 204, or insertion of the text to the inside of the main part 208 of the message 204. The execution mode of notes action is based on the policy inputted by the administrator. The notice action 616 produces transmission of one or two notices or more of E-Mail, when the trigger of the given policy is carried out. A notice can be transmitted to the E-Mail address specified by the sending person, the addressee, the administrator, or the administrator. In addition, the notice action 616 enables description about whether the original message 204 should be attached to a notice. The treatment action 620. [that it should be continued whether sending a message to a destination (specified by the destination field 206), and] Or it is judged whether one of two or more alternative actions 622 (adjournment of a message, isolation, return to a sending person, a stop, etc.) is required.

[0031]

The step shown in drawing 6 (b) is performed for each [which was specified about the message 204] destination of every. The step shown in drawing 6 (b) is performed about the message generated by Step 622 again. To the 1st, the policy manager 216 performs action 610,612,614,616 for each [which is specified in the message 204] destination of every. The processing action 623. [that it should be continued whether sending a message to a destination (specified by the destination field 206), and] Or by judging whether it needs one or postponing of two or more alternative actions 622, it operates like the treatment action 620 (adjournment of a message, isolation, return to a sending person, the stop, etc.). It is judged at Step 624 whether encryption of a message is required. When encryption of a message is required, according to the key 628 stored, encryption is performed at Step 626. When encryption of a message is not required, a message is transmitted to the specified destination at Step 630. The message processed by the block 622 is checked at Step 624 before transmission. For example, the message which is postponed, and is isolated or is returned to a sending person may need encryption.

[0032]

Drawing 7 is a block diagram showing the alternative action 622 still in detail. The message which received from the treatment step 620 is stored in one of the four queuing 702 including the isolation queuing 704, the retry queuing 706, the dead letter queuing 708, and the adjournment queuing 709 according to the specified message treatment. The isolation queuing 704 stores a message in preparation for following extraction and examination by human being who has a system administrator and other authority. The retry queuing 706 stores the message which failed in distribution. Transmission of the message in the retry queuing 706 is retried behind. After a some times retry, the dead letter queuing 708 is non-delivery, and stores continuously the message which cannot be returned to a sending person, either. The message in the dead letter queuing 708 will be processed by the system administrator. The adjournment queuing 709 stores the message which delays a stage and should be distributed automatically (to for example, time which removed the peak period term, such as a weekend or night). The composition module 230 provides two or more actions 710-714 which can be performed about the message in the queuing 702. A sending person is returned [what an administrator looks at a message for (block 710)] (block 711), It is possible to delete (block 712), to send to one or more specified destinations (block 713), and/or to save (block 714).

[0033]

It will be understood that an above-mentioned specific mechanism and art only illustrate the example of 1 application of the principle of this invention. It is possible to add various corrections to above method and device, without deviating from the true technical idea and range of this invention.

[Brief Description of the Drawings]

[Drawing 1]

It is a block diagram showing two or more E-Mail networks which use the E-Mail firewall which was connected via the Internet and adopted the principle of this invention.

[Drawing 2]

It is a block diagram showing the suitable embodiment of an E-Mail firewall.

[Drawing 3]

It is a block diagram showing operation of the E-Mail firewall of drawing 2 in details more.

[Drawing 4]
It is a block diagram showing operation of the E-Mail firewall of drawing 2 in details more.
[Drawing 5 (a)]
It is a block diagram showing an alternative safe E-Mail transmitter style.
[Drawing 5 (b)]
It is a block diagram showing an alternative safe E-Mail transmitter style.
[Drawing 5 (c)]
It is a block diagram showing an alternative safe E-Mail transmitter style.
[Drawing 6 (a)]
It is a flow chart which shows operation of the suitable embodiment of an E-Mail firewall.
[Drawing 6 (b)]
It is a flow chart which shows operation of the suitable embodiment of an E-Mail firewall.
[Drawing 7]
It is a block diagram showing the portions of drawing 6 (a) and drawing 6 (b) much more in detail.

[Description of Notations]

105 The E-Mail firewall 202. Field of SMTP relay module 204-message 205 source-field 206 destination field 207 subject-field 208 main part 209 attachment field 210 The internal site 212. External site 214 policy engine 216 policy manager 218 access-manager 220 contents manager 222 format manager 224 virus manager 226 security manager 230 Composition module

---

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]
An E-Mail control system characterized by comprising the following for controlling an E-Mail message which was transmitted from a computing site or was received by computing site.
A message encoding means which enciphers a message of a type with which the 1st transmitted was specified according to an encryption key with which the at least one 1st was stored from said computing site.
A message decryption means which deciphers a message of a type with which the 2nd received by said computing site was specified according to an encryption key with which the at least one 2nd was stored.
A filter which supervises a message according to filter information which can be changed before encryption after decryption by this message decryption means, and by said message encoding means.

[Claim 2]
The E-Mail control system according to claim 1 with which said filter restricts transmission of a message in which this contents filter includes information corresponding to contents filter information in which the change is possible including a contents filter.
[Claim 3]
Each of said message has the destination information which identifies 1st at least one destination about this message, The E-Mail control system according to claim 2 with which said filter restricts transmission of a message in which this destination filter includes information corresponding to destination filter information in which the change is possible including a destination filter.
[Claim 4]

Each of said message has a source information which identifies 1st at least one sauce about this message, The E-Mail control system according to claim 3 with which said filter restricts transmission of a message in which this sauce filter includes information corresponding to sauce filter information in which the change is possible including a sauce filter.

[Claim 5]

The E-Mail control system according to claim 4 provided with a means to make a message including information corresponding to filter information in which said change is possible transmit to a different destination from said 1st destination at least of this message according to said filter.

[Claim 6]

The E-Mail control system according to claim 5 provided with a means to make a message including information corresponding to filter information in which said change is possible transmit to a destination corresponding to said 1st destination of this message at least according to said filter.

[Claim 7]

An E-Mail control system comprising:

A reporting means which makes an E-Mail notification message generate according to said means to make said message transmit.

A transfer means which makes said E-Mail notification message transmit to a destination corresponding to notification message destination information which can be changed.

[Claim 8]

The E-Mail control system according to claim 7 with which said notification message has a body part, and said reporting means is provided with a means to make a message contained in said body part generate.

[Claim 9]

An E-Mail firewall characterized by comprising the following for processing an E-Mail message transmitted between one internal site and two or more external sites.

An E-Mail relay which transmits an E-Mail message which is not sifted out from the 1st external site, receives an E-Mail message enciphered, and is sifted out, and is enciphered to the 2nd external site.

According to said enciphered E-Mail message which received from said 1st external site and which is not sifted out, Decipher this message and a message which is not sifted out and enciphered is generated according to a key with which the 1st is stored, It is sifted out and said E-Mail message which is sifted out and is not enciphered is enciphered according to a key with which the 2nd is stored according to an E-Mail message which is not enciphered, A security manager who generates said E-Mail message which is sifted out and enciphered.

According to said E-Mail message which was generated by said security manager and which is not sifted out and enciphered, An E-Mail message [this] which is not sifted out and enciphered is sifted out according to policy information stored, An E-Mail message which is sifted out and is not enciphered, It generates for the 1st internal site specified by this E-Mail message which is sifted out and is not enciphered, Corresponding [and] to an E-Mail message which is not sifted out from the 2nd internal site and is not enciphered, An E-Mail message [this] which is not sifted out and enciphered is sifted out according to said policy information stored, A policy manager who generates said E-Mail message which is sifted out and is not enciphered for said security manager.

[Claim 10]
Transmission of an E-Mail message between the 1st one site and two or more 2nd sites, It is an E-Mail firewall for restricting according to two or more policies which can be chosen by an administrator, An SMTP (Simple Mail Transfer Protocol) relay for making said E-Mail message transmit between said 1st site and a site where it was chosen of said 2nd site, Are a policy manager who performs compulsorily two or more policies which can be chosen by an administrator according to said SMTP relay, and said policy The 1st at least one sauce / destination policy, Two or more standards which it has 1st at least one contents policy and 1st at least one virus policy, and can be chosen by this policy by an administrator, Have a policy manager who is what is characterized by two or more exceptions which receive said standard which can be chosen by an administrator, and two or more actions in relation to said standard which can be chosen by an administrator, and said exception, and this policy manager, An access manager who restricts transmission of an E-Mail message between said 1st site and said 2nd site according to said sauce / destination policy, A contents manager who restricts transmission of an E-Mail message between said 1st site and said 2nd site according to said contents policy, An E-Mail firewall provided with a virus manager who restricts transmission of an E-Mail message between said 1st site and said 2nd site according to said virus policy.
[Claim 11]
The E-Mail firewall according to claim 10 provided with a format manager who changes said E-Mail message into the 2nd format from the 1st format according to said policy which can be chosen by an administrator by said policy manager.
[Claim 12]
Said E-Mail message is formatted into two or more fields, The field of this plurality A source field, the destination field, the E-Mail firewall according to claim 10 to which said access manager answers said sauce / destination policy specified for every each of said field of said E-Mail message including a subject field and message fields.
[Claim 13]

An E-Mail firewall given in a claim to which said E-Mail message is characterized by a size field, and said access manager answers said sauce / destination policy specified about this size field.

[Claim 14]

The E-Mail firewall according to claim 12 which said E-Mail message is characterized by a date and the time field, and answers said sauce / destination policy as which said access manager was specified about this date and the time field.

[Claim 15]

The E-Mail firewall according to claim 10 from which said virus manager detects a virus contained in information this compressed according to an E-Mail message including compressed information.

[Claim 16]

The E-Mail firewall according to claim 12 to which said contents manager answers information included in said subject field and said message fields according to said contents policy.

[Claim 17]

The E-Mail firewall according to claim 16 to which said E-Mail message answers attached information by which said contents manager was specified as said attachment field according to said contents policy including the attachment field.

[Claim 18]

It is a method for restricting transmission and reception of an E-Mail message between the 1st one site and two or more 2nd sites according to a policy in which two or more change is possible, The 1st E-Mail message transmitted between at least one of said 1st site and said 2nd sites is monitored, When it judges whether said message is enciphered and this message is enciphered, said message is deciphered according to a key stored -- a method for restricting transmission and reception of an E-Mail message which has each step of filtering said message according to two or more policies stored.

[Claim 19]

The 2nd E-Mail message transmitted between 1 of said 2nd sites and said 1st site is monitored, This E-Mail message is filtered according to two or more policies stored, A method according to claim 18 of having further each step of enciphering said E-Mail message according to said key stored according to the 1st policy of said policies stored, and transmitting this E-Mail message to said 1st site.

[Claim 20]

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL FIELD

[Field of the Invention]
Especially this invention relates to the security for an electronic mail system, concerning the computer security field generally.
[0002]

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

PRIOR ART

[Description of the Prior Art]
The new way for operating level communication and electronic commerce technology (EC) was cut by the E-mail (E-Mail) accompanying growth and omnipresence of the Internet, and the extensive use of groupware. An organization comes to be dependent on E-Mail which passed the Internet for transmission of important files, such as a purchase order in an in-house, a sales forecast, financial information, and a contract, gradually, and has come to be dependent on E-Mail gradually also among different organizations for the same processing. In such a situation, those files serve as important property which must be protected.
[0003]
In order to guarantee the present-day confidentiality and integrity of data communications, many security references exist conventionally. For example, the conventional firewall prevents network access by a user without authority. Secure socket art (Secure Socket Technology) makes it possible to send data safely via World Wide Web (WWW). However, a problem still has much E-Mail which is the use on the Internet projected most in respect of security for almost all organizations. Many conventional firewalls restrict access to the information only protected by this firewall.
It does not have the capability to restrict transmission of the information on the outside of the in-house by E-Mail.
This passes to the viral infection by accidental or intentional disclosure of the extra sensitive information by E-Mail being emitted from an in-house, and E-Mail included in an in-house.
[0004]
Encryption of this message is mentioned as one method for protecting airtightness or an E-Mail message. Security can be obtained by the digital signature which provides attestation of an E-Mail message. Each of encryption and attestation is supported with the S/MIME (Secure/Multipurpose Internet Mail Extensions) messaging protocol. This protocol, By IETF

(International Engineering Task Force). The document it is ["S/MIME Message Specification" (1997) and "S/MIME Certificate Handling" (1997) which were published] entitled is specified. Each user can carry out encryption / decryption, and attestation of an E-Mail message using commercial software. However, implementation of this work that uses software will not restrict with an always simple thing, but, so, the ease of original use of E-Mail as a means of communication may be spoiled. The organization which desires to use this software has to leave encryption of all the needed messages to each user, without having a means for performing CC in any way. In addition, many conventional firewalls do not have the capability to control the contents or form of a fixed message of frequenting an organization. For example, many conventional firewalls do not have the capability to guarantee that E-Mail is meeting the fixed standards, like contents or sauce and/or the destination address, or the domain is enciphered. Many conventional firewalls do not have the capability to control the message which is not desirable as for the E-Mail advertisement included in an in-house etc. which are not welcomed.

[0005]

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention]
Therefore, the E-Mail firewall which provides the improved CC to the E-Mail message which goes in and out to an organization is needed.
[0006]

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

MEANS

[Means for Solving the Problem]
In a main mode, this invention provides an E-Mail firewall (105) which sifts out an E-Mail message (204) which occurs within a computer network (101,103) or enters into the network. An embodiment which adopted a principle of this invention takes advantageously a form of an E-Mail control system (105) which controls an E-Mail message (204) transmitted and received between computing sites. This E-Mail control system (105) is provided with a message encoding means (526) which enciphers a message (204) of a type with which the 1st transmitted from a computing site was specified according to an encryption key (528) with which the at least 1st was stored. A code of a message (204) of a type with which the 2nd by which a message decryption means (552) was received by computing site according to an encryption key (528) with which the at least 2nd was stored was specified
It decodes. A filter (216) supervises a message (204) according to filter information (216) which can be changed before encryption after decryption by said message decryption means (552), and by said message encoding means (526).
[0007]
There is an important advantage of this embodiment in CC of an E-Mail policy by an organization increasing. All the E-Mail messages generated in entering or an in-house can be enciphered or deciphered according to a policy on which it was imposed by organization to an in-house, and it can filter. For this reason, each user of a desktop computer of an in-house does not need to be concerned with following an E-Mail policy of this organization certainly. An E-Mail message can be supervised about sauce or a destination specific about specific contents.
[0008]
An embodiment which adopted a principle of this invention also advantageously acts as a transparent existence to each user of an in-house. For example, each user of this does not

need to be concerned with following an encryption policy of an organization. It can encipher automatically and/or an E-Mail message which is emitted from an E-Mail message including specific contents, a specified address, or a domain, or is transmitted to this address or a domain can be filtered. For example, other organizations (for example, the company B) and an organization (for example, the company A) which exchanges E-Mails frequently, When it is judged that all the E-Mails to the company B should be enciphered on security, it is possible to build an E-Mail firewall in the above companies A, and to recognize a domain name of the company B, and to store an encryption key. It will be enciphered by above-mentioned E-Mail firewall, without all the E-Mail messages to the company B needing additional operation by each user from the company A after that. When the company B has already built an E-Mail firewall which adopted an above-mentioned principle, this E-Mail firewall can be built so that a message from the company A may be deciphered. Therefore, each addressee in the company B which received E-Mail from the company A does not need to perform additional operation, in order to decipher E-Mail from the company A. Therefore, all the E-Mail messages to the company B become possible [exchanging without an intervention by a user certainly also in the company A or the company B] from the company A. Of course, an E-Mail firewall of the company B can be constituted so that same E-Mail message transmission to the company A may become possible from the company B.

[0009]

It is possible to carry out another policy to message transmission between the companies A and B. For example, by constituting using a rule which recognizes an E-Mail message which contains a specific term or a phrase for an above-mentioned filter of the target E-Mail firewall, and prevents the transmission, It is possible to reduce accidental (or it is intentional) disclosure of specific information between the companies A and B. An E-Mail firewall can also be constituted again so that an exception over this rule may be used. For example, it is possible to carry out E-Mail from a specific user or E-Mail to a specific user outside of an object of application of this rule. After transmission of a message is prevented, operation performed by E-Mail firewall can be changed. For example, it is possible to return a message which poses a problem to a sending person with an explanation message. In order that an administrator may see alternatively in addition to the above, it is possible to store the message concerned or to delete this message. (It relates to one, or two domains or each addresses or more, respectively) Many encryption keys can be stored in an E-Mail firewall which adopted an above-mentioned principle, and many domains and/or safe communication with each user can be enabled.

[0010]

**** and other advantages of this invention will be further understood by fitness by referring to the following detailed explanation.

[0011]

[Embodiment of the Invention]

In drawing 1, the E-Mail network 101,102 is connected to the E-Mail network 103 via WAN (Wide Area Network) 104, such as the Internet. Between the Internet 104 and the E-Mail network 101,103, the access firewall 106 and the E-Mail firewall 105 are allocated. The E-Mail network 102 is connected to the Internet 104 by only the access firewall 106. The E-Mail network 101,102,103 takes the conventional gestalt, respectively. For example, the E-Mail networks 101-103 can take the form of two or more LAN which supports one LAN (Local Area Network), one, or two conventional E-Mail messaging protocols or more. The access firewall 106 can also take the conventional gestalt. The access firewall 106 operates so that access to the file from the machine arranged in the remote place stored in the computer network (the E-Mail network 101 - 103 grades) may be restricted. The E-Mail firewall 105 (the numerals 105.1 and 105.2 show separately) can take advantageously the form where it explains in detail in this book, in order to control transmission of the E-Mail message between one internal site, one, or two external sites or more. For example, one internal site about the E-Mail firewall 105.2 can take the form of the E-Mail network 103. The external sites about the E-Mail firewall 105.2 are all sites that are not included in the E-Mail network 103. For example, the external sites about the E-Mail firewall 105.2 are the arbitrary sites in the E-Mail network 101,102, and all sites of the others connected to the Internet 104. The E-Mail firewall 105 is arranged suitably at the access firewall 106 "safe side." Drawing 1 should be understood as what shows the principle of the embodiment written in this book, for example. The access firewall 106 is not required for operation of the embodiment which was shown for the purpose of illustrating this invention and adopted the principle of this invention.

[0012]

Suitably, the E-Mail firewall 105 takes the form of the program executed on the conventional general purpose computer. Windows NT available [with a typical embodiment] from Microsoft Corporation (Redmond, Washington) in a computer An operating system (trademark) is performed. Although the E-Mail firewall 105 is shown by drawing 1 as what operates about an E-Mail message between an internal site and an external site, It is also possible to use this E-Mail firewall 105 and to exchange messages between two internal sites of two or more computer networks which have the messaging backbone according to SMTP.

[0013]

The block type showing the main functional components of the E-Mail firewall 105.1,105.2 shows drawing 2. In the figure, the SMTP (Simple Mail Transfer Protocol) relay module 202 achieves the conventional Internet relay host's function. The Internet relay host's example is a sendmail program. The SMTP relay module 202 transmits and receives an E-Mail message (the numerals 204 show) between the internal site 210 and the external site 212. The E-Mail message 204, The E-Mail address of the sauce of this message 204. The destination field 206 which specifies one or two destination E-Mail addresses or more, the source field 205 and this message 204, to specify, the subject field 207 which specifies the title (namely, subject) of this message 204, . Called it the attachment field 209 which specifies one or two files or more which should transmit with the field 208 of a main part which specifies the main part (a text and/or graphics data are included) of this message 204, and this message 204. The form of the conventional E-Mail message including two or more user appointed information fields is taken. Although the priority of a message, a transmitting side agent's identifier, and the time of a message are mentioned as the other user appointed fields, the user appointed field is not limited to these.

[0014]

The E-Mail message 204 can be encoded according to one of two or more encoding forms which are explained in full detail below. As for the SMTP relay module 202, it is preferred to take the form of the conventional software module which transmits and receives an E-Mail message according to the SMTP protocol specified by Internet RFC821. An SMTP protocol is not important for this invention, and in other examples. It is possible to transpose an SMTP relay module to the module which transmits and receives a message in another forms, such as FTP (File Transfer Protocol) or HTTP (Hyper-Text Transfer Protocol).

[0015]

As for the SMTP relay module 202, it is preferred to be constituted so that it may opt for routing to the addressee of a message using DNS (Domain Name System), It is possible to relay a message to the SMTP host specified by the administrator alternatively. When DNS is chosen, the default SMTP host can still specify, in order to enable transmission of a message, even if it is a case where DNS service cannot be used. The routing option can carry out an override per domain. The SMTP relay module 202 makes it possible to make it possible going up between also advantageously specific hosts, or to get down and to restrict SMTP connection of a direction for things, and to refuse connection between specific SMTP hosts.

[0016]

Drawing 3 shows the mode in which the message from the internal site 210 and the external site 212 received with the SMTP relay module 202 is processed by the policy engine 214. The policy engine 214 receives the message from the SMTP relay module 202, It judges which policy is applicable to this message by creating the list 302 of sending person policies about the sending person (sauce) 205 of this message, and creating the list 304,306,308 of addressee policies for every addressee. Subsequently, the policy engine 214 calls the policy manager 216, in order to apply each policy. The policy of a different type has a predetermined priority about the application. For example, a code release policy is applied before other policies, and it enables the policy which acts about the field 208 of a main part of a message to access by this the contents included in this main part. At an alternative embodiment, the turn that a policy is applied can be chosen by a system administrator. An access manager policy is applied after a decryption policy, and, subsequently other policy managers are repeatedly called in the turn suggested by the policy which should be applied to a message. Subsequently, the policy engine 214 receives the result from a policy manager, and transmits a message to the SMTP relay module 202 according to the this received result. The result received with this policy engine 214 comprises actions explained in full detail in this book, such as treatment, notes, and a notice. The processing result of the message 204 with the policy engine 214 generates two or more additional messages (for example, notice to a sending person, an addressee, or a system administrator). According to a suitable embodiment, the policy engine 214 is carried out as a program executed with a digital computer.

[0017]

The policy manager 216 can operate so that forcible execution of the policy inputted by the administrator of the E-Mail firewall 105 may be carried out. As for the policy manager 216, it is preferred to comprise two or more modules for carrying out forcible execution of the policy constituted by the administrator for the E-Mail message of a specific form. For example, in the E-Mail firewall 105 the policy manager 216, Two or more manager modules including the access manager 218, the contents manager 220, the format manager 222, the virus manager 224, and the security manager 226 are carried out. As for the policy manager 216, it is preferred to be developed by the input inputted by the administrator via the composition module 230. According to the information inputted by the administrator, the composition module 230 operates again so that the SMTP relay module 202 and the policy engine 214 may be constituted. The policy manager who shows drawing 2 and explains here used to aim only at illustration of a model embodiment. It also has intention of the policy manager of other types as a thing in a principle given in this book.

[0018]

The access manager 218 provides compulsive execution of access control policies, such as a destination to which transmission of E-Mail was forbidden, or sauce which cannot receive E-Mail. The access manager 218 can filter the message exceeding the maximum message size determined by the administrator again, or the message which includes a specific word all over the subject field 207. The access manager 218 can also filter a message with the priority of the message specified by the user. For example, while sending the message of a high priority promptly so that drawing 7 may be explained in full detail below, it is possible to put the message of a low priority into queuing. The access manager 218 can filter a message by the transmission date and/or time of a message again. For example, the message transmitted to the specific time zone of the one day or the specific day (for example, a weekend or a holiday) can carry out the maintenance or further filtering (for example, contents manager 220).

[0019]

The contents manager 220 supports compulsive execution of a contents control policy. Suitably The word in the field 208 of (a) main part with the specific contents manager 220, (b) Support filtering by 1 of the standards of the specific word in the subject field 207 or the field 208 of a main part, and (c) attachment field 209 (the all, or a name/type), or two or more. A contents control policy and other suitable policies can be specified that it needs a specific material (for example, a specific notice or refusal). The virus manager 224 supports compulsive execution of a virus control policy by detecting the E-Mail attached file infected with the virus. As for the virus manager 224, it is preferred to detect the virus contained in the compressed file format of the plurality containing PKZip, PKLite, ARJ, LZExe, LHA, and MSCompress. For example, the virus manager 224 can use a commercial virus scan engine. As for the virus manager 224, it is preferred to apply a policy again to "a clean message, i.e., the message the virus scan being carried out and not being infected with a virus turns out to be." The "clean stamp" notes which show that a virus was not detected are given to this message.

[0020]

The format manager 222 provides conversion of the E-Mail message to the 1st format [2nd] from a format. According to a suitable embodiment, the format manager 222 changes a message into a MIME format from a UUENCODE format. Suitably, the format manager 222 changes a message in advance of the message processing by other policy managers.

[0021]

As for the security manager 226, it is preferred to carry out forcible execution of two or more E-Mail encryption policies. Suitably, the security manager 226 does forcible execution of a client security use policy, a code protection policy, a plain text access policy, and the default action policy. The security manager 226 applies again the proxy encryption and the signature policy which are explained in full detail below in relation to drawing 5 (b) instead of a user.

[0022]

A client security use policy specifies what a specific user should perform encryption or a signature for by a desktop. In order to show the time when forcible execution of this policy should be carried out, it is possible to set up an additional standard. For example, it is possible to specify E-Mail to the lawyer of a company from CEO of the company by the domain or a full E-Mail address as what needs encryption or a signature, and to carry out forcible execution of the representative-client privilege, and to suspend an encryption policy. What the message which uses a client security use policy, is already in encryption form, and probably meets other standards should be saved for (if it puts in another way) It is possible to specify what processing by the E-Mail firewall 105, correction, or decryption is not performed for. A plain text access policy needs to design the E-Mail firewall 105 as an addressee of a message by whom the specific type was specified. The E-Mail firewall 105 is specified as an addressee of an encryption message, in order to apply access, contents, a virus, and other policies to a message. A plain text access policy can be used in order to send the notice with a signature to the sending person of a message again as one method of providing the sending person of a message with the public key of the E-Mail firewall 105. A default action policy is a message which is not enciphered, and it shows action which should be performed about the optional message which meets other standards of a certain selectively, without being enciphered by the E-Mail firewall 105. This policy type is used in order to ensure that a specific message is enciphered by somewhere (a desktop or E-Mail firewall 105).

[0023]

As for a policy, it is preferred to be inputted by the permitted administrator via the composition module 230, and, as for this composition module 230, it is preferred to take the form of the program executed on the computer by which the program was stored. A policy can be individually applied advantageously by the group of an E-Mail domain or others to a user. Drawing 4 shows the mode to which a policy is applied. The user can compose of hierarchy-like directory structure so that the grouping of a user and/or a domain may become easy. When a policy is applied to a given directory, the policy which requires the subdirectory corresponding to a directory given [this] is inherited. For example, in drawing 4, the policy 1 is applied to the subdirectory 404 and applied to all the subdirectories, a domain, and a user (for example, the subdirectory 412, the user 408, and the domain 410) by extension. This is performed unless the override of this policy is clearly carried out by another policy applied to the specific subdirectory or the intervening subdirectory. For example, about the user 1 (the numerals 408 show), the policy 3 carries out the override of the policy 1, when competition exists between this policy 3 and the policy 1, and when competition does not exist, it will compensate the policy 1. The exception 1 will carry out the override of the policies 1 and 3 about the specific exception specified with the exception 1. As shown in drawing 4, the policy 1 is applied to the user 414,416,418, when competition exists, the override of it is carried out by the policy 2 about the user 414,416,418, and when competition does not exist, it will supplement. Thereby, it becomes also advantageously possible to apply a policy to an user group easily. However, the exact mode in which a policy is stored is not important for this invention, and it is possible to adopt various storing means and storing form.

[0024]

The E-Mail message 204 which was received by the SMTP relay module 202 and/or was transmitted, By IETF (Internet Engineering Task Force). S/MIME (Secure/Multipurpose.) specified in the document it is ["S/MIME Message Specification" (1997) and "S/MIME Certificate Handling" (1997)] entitled It is preferred to be encoded according to an Internet Mail Extension protocol. To an advantageous thing, this S/MIME protocol, Security is built by the top layer of an engineering specification MIME protocol according to RSA Data Security and Public Key Cryptography Standards (PKCS: public-key-encryption-ized standard) specified by Inc. Also advantageously, S/MIME provides the security service about the privacy using the attestation and encryption which used the digital certificate. A digital certificate, Also as "the ITU-T recommendation X.509" (June, 1997). "It is known Information Technology. - It is preferred to carry out according to the X.509 format specified by Open Systems Interconnection - The Directory:Authentication Framework." As for encryption, it is preferred that one of symmetrical encryption algorithm DES, Triple-DES, and RC2 performs. It is a well-known thing, and the S/MIME protocol is used widely, provides encryption and a digital signature, and is [therefore] preferred as a communications protocol. However, the details of operation of this protocol are not important for this invention. It will be understood that it is also possible to use other safe messaging protocols called PGP (Pretty Good Privacy) or OpenPGP specified by the ITF workgroup.

[0025]

The access manager 218 is a policy manager of the beginning for processing the E-Mail message 204. The access manager 218 acts only about the message header information which is not enciphered. For this reason, the access manager 218 processes the E-Mail message 204 in advance of decryption with the S/MIME engine 215. Generally the term "message header information" points out the portion except the field 208 (generally called a message text) of a main part, and the attachment field 209 among messages. Therefore, header information includes a source field, the destination field, and a subject field (205,206,207). As other fields which can be contained in a message header, a date / time stamp, a priority, and a transmitting side agent are mentioned. The remaining modules act on the message 204 after processing with the S/MIME engine 215. As for the format manager 222, like previous statement, it is preferred to act on a message in advance of the operation by other managers, such as the virus manager 224, the security manager 226, and the contents manager 220.

[0026]

An S/MIME protocol makes it possible to exchange the E-Mail message 204 with two safe sites which support an S/MIME protocol. When a transmitting site and a receiving site perform an S/MIME function, a virtual private network (VPN) as shown in drawing 5 (a) can be attained. VPN (here, "object level E-MailVPN" is called) obtained as a result provides encryption / signature of the message between a transmitting site and a receiving site, and/or decryption/verification. In object level E-MailVPN shown in drawing 5 (a), it is enciphered separately and each object (message) is sent via a standard (SMTP) transmission medium. In this case, each object is deciphered by the other end. This object level E-MailVPN does not need the safe real-time connection needed by the conventional VPN for an advantageous thing. As shown in drawing 5 (a), the mail server 105.1,105.2 performs the function explained in this book about the E-Mail firewall 105, and object level E-MailVPN is attained among them as the result. E-Mail enciphered and transmitted with 105.1,105.mail server 2 admiration, After passing the server with huge E-Mail transmitted via the Internet 104 which is not safe, in spite of the fact of reaching the destination (namely, address), it is protected from the indication to a third party. In this exchange, the E-Mail firewall 105.1,105.2 provides generation of the key of a couple, and a key certificate, and provides exchange of the public key certification in automatic or hand control with other S/MIME servers. In addition, the E-Mail firewall 105.1,105.2 enables selection of discernment of other S/MIME servers through a directory domain record, the combination of a directory domain record with a server certificate, encryption/signature algorithm, and key length. The directory domain record and the directory user record explained below are indicated to drawing 4.

[0027]

Exchange of the message encoded [S/MIME] can also be performed again between the E-Mail firewall 105.1,105.2 and the S/MIME client connected to the server which does not perform an S/MIME function. Drawing 5 (b) shows the data exchange between the S/MIME clients connected to the E-Mail firewall 105 and the non-S/MIME server 506. In drawing 5 (b), the server 105.1 performs encryption and decryption of a message instead of the client 502, and, generally provides the above-mentioned function about the E-Mail firewall 105.1,105.2. In detail, in this exchange, the E-Mail firewall 105.1 provides generation of the key of a couple, and a public key certification, and provides exchange of the public key certification in automatic or hand control with the client 508.1. In addition, the E-Mail firewall 105.1 enables selection of discernment of the client 508.1 through a directory user record, the combination of a directory user record with an user certificate, encryption/signature algorithm, and key length. The client 508.1 provides encryption/decryption service, in order to make it possible to transmit a message safely via the server 506 by supporting encryption/decryption service. In drawing 5 (b), object level VPN (here, "proxy security" is called) specific type is attained between the server 105.1 and the client 508.1. In proxy security, at least one client (client 508.1 grade in drawing 5 (b)) is concerned with execution of encryption/decryption. The encryption/code in which this is performed by the server 105.1,105.2

It is contrastive with the composition of drawing 5 (a) where decipherment service is not in sight from the client 502.1,502.2.

[0028]

In drawing 5 (a), although the communication between the servers 105.1,105.2 is safe, the communication between the client 502.1,502.2 and each server 105.1,105.2 is not safe. In the equipment which many require, security is unnecessary. However, when this security is desired, it is possible to mount encryption/decryption service also in the client 508.1,508.2, and to perform proxy security. The server 105.1,105.2 in drawing 5 (c) performs the same function as what was mentioned above about drawing 5 (a), therefore attains object level VPN. In addition, the client 508.2,508.1 enables safe communication between the corresponding servers 105.1,105.2. The encryption/decryption performed by the server 105.1,105.2 should care about that it is possible to have become independent of the encryption performed by the corresponding client 508.2,508.1. For example, the message from the client 508.2 to the client 508.1, It is enciphered at the time of transmission to the server 105.1, and is deciphered by the server 105.1, Receive suitable action by a policy manager and, subsequently to [for transmission to the server 105.2], it is enciphered, This client 508.1 is able to be deciphered by the server 105.2, to receive suitable action by a policy manager, to be enciphered subsequently to [for transmission to the client 508.1], and to decipher a message. Alternatively the message from the client 508.2 to the client 508.1, It is enciphered by the client 508.2 and suitable action to non-enciphering portions (destination field etc.) is received, Subsequently, it is again enciphered by the server 105.1 for the transmission to the server 105.2 of the whole (the portion which is not enciphered by the client 508.2 is included) message, In order that this server 105.2 may decode encryption by the server 105.1 and may decode the encryption performed by the client 508.2, it is possible to transmit a message to the client 508.1. The combination of the two above-mentioned scenarios is also feasible.

[0029]

Each E-Mail message 204 processed by the E-Mail firewall 105 is processed according to the step shown in drawing 6 (a) and drawing 6 (b). Drawing 6 (a) is a flow chart which shows operation of the E-Mail firewall 105 according to the message which received. Drawing 6 (b) is a flow chart which shows operation of the E-Mail firewall 105 before transmitting a message. The message processed by the E-Mail firewall 105 may receive from an external site, in order to receive from an internal site in order to receive from an internal site in order to transmit to an internal site, or to transmit to an external site, or to transmit to an internal site. All single messages can include an inside and the external destination 206. The step shown in drawing 6 (a) and drawing 6 (b) is performed by generating the sending person policy and addressee policy which are shown in drawing 3. therefore, for every each of two or more destinations, the step shown in drawing 6 (b) can be performed variously, and it has a different result for every different destination.

[0030]

Drawing 6 (a) is referred to here. At Step 602, it is judged whether decryption of the portion of the message 204 is required for the E-Mail firewall 105. When decryption is required, according to the key 628 stored, decryption is performed at Step 604. After this decryption when decryption is unnecessary, The E-Mail firewall 105 applies the policy manager 216, and this policy manager 216 performs action (Step 610,612,614,616 shows) of four types to the E-

Mail message 204. The standard action 610 provides a filtering reference with the selected administrator. The exception action 612 judges which standard 610 is excepted. It will be possible to choose two or more standards 610, and the logic AND operation of a standard will arise as a result. It will be possible to choose two or more exceptions 612, and an exceptional logic OR operation will arise as a result. That is, the trigger of the policy will be carried out to any one of exception conditions being truth. The notes action 614 produces generation of the attachment field to the message 204, or insertion of the text to the inside of the main part 208 of the message 204. The execution mode of notes action is based on the policy inputted by the administrator. The notice action 616 produces transmission of one or two notices or more of E-Mail, when the trigger of the given policy is carried out. A notice can be transmitted to the E-Mail address specified by the sending person, the addressee, the administrator, or the administrator. In addition, the notice action 616 enables description about whether the original message 204 should be attached to a notice. The treatment action 620. [that it should be continued whether sending a message to a destination (specified by the destination field 206), and] Or it is judged whether one of two or more alternative actions 622 (adjournment of a message, isolation, return to a sending person, a stop, etc.) is required.

[0031]

The step shown in drawing 6 (b) is performed for each [which was specified about the message 204] destination of every. The step shown in drawing 6 (b) is performed about the message generated by Step 622 again. To the 1st, the policy manager 216 performs action 610,612,614,616 for each [which is specified in the message 204] destination of every. The processing action 623. [that it should be continued whether sending a message to a destination (specified by the destination field 206), and] Or by judging whether it needs one or postponing of two or more alternative actions 622, it operates like the treatment action 620 (adjournment of a message, isolation, return to a sending person, the stop, etc.). It is judged at Step 624 whether encryption of a message is required. When encryption of a message is required, according to the key 628 stored, encryption is performed at Step 626. When encryption of a message is not required, a message is transmitted to the specified destination at Step 630. The message processed by the block 622 is checked at Step 624 before transmission. For example, the message which is postponed, and is isolated or is returned to a sending person may need encryption.

[0032]

Drawing 7 is a block diagram showing the alternative action 622 still in detail. The message which received from the treatment step 620 is stored in one of the four queuing 702 including the isolation queuing 704, the retry queuing 706, the dead letter queuing 708, and the adjournment queuing 709 according to the specified message treatment. The isolation queuing 704 stores a message in preparation for following extraction and examination by human being who has a system administrator and other authority. The retry queuing 706 stores the message which failed in distribution. Transmission of the message in the retry queuing 706 is retried behind. After a some times retry, the dead letter queuing 708 is non-delivery, and stores continuously the message which cannot be returned to a sending person, either. The message in the dead letter queuing 708 will be processed by the system administrator. The adjournment queuing 709 stores the message which delays a stage and should be distributed automatically (to for example, time which removed the peak period term, such as a weekend or night). The composition module 230 provides two or more actions 710-714 which can be performed about the message in the queuing 702. A sending person is returned [what an administrator looks at a message for (block 710)] (block 711), It is possible to delete (block 712), to send to one or more specified destinations (block 713), and/or to save (block 714).

[0033]

It will be understood that an above-mentioned specific mechanism and art only illustrate the example of 1 application of the principle of this invention. It is possible to add various corrections to above method and device, without deviating from the true technical idea and range of this invention.

[Brief Description of the Drawings]

[Drawing 1]

It is a block diagram showing two or more E-Mail networks which use the E-Mail firewall which was connected via the Internet and adopted the principle of this invention.

[Drawing 2]

It is a block diagram showing the suitable embodiment of an E-Mail firewall.

[Drawing 3]

It is a block diagram showing operation of the E-Mail firewall of drawing 2 in details more.

[Drawing 4]

It is a block diagram showing operation of the E-Mail firewall of drawing 2 in details more.

[Drawing 5 (a)]

It is a block diagram showing an alternative safe E-Mail transmitter style.

[Drawing 5 (b)]

It is a block diagram showing an alternative safe E-Mail transmitter style.

[Drawing 5 (c)]

It is a block diagram showing an alternative safe E-Mail transmitter style.

[Drawing 6 (a)]

It is a flow chart which shows operation of the suitable embodiment of an E-Mail firewall.

[Drawing 6 (b)]

It is a flow chart which shows operation of the suitable embodiment of an E-Mail firewall.

[Drawing 7]

It is a block diagram showing the portions of drawing 6 (a) and drawing 6 (b) much more in detail.

[Description of Notations]

105 The E-Mail firewall 202. Field of SMTP relay module 204-message 205 source-field 206 destination field 207 subject-field 208 main part 209 attachment field 210 The internal site 212. External site 214 policy engine 216 policy manager 218 access-manager 220 contents manager 222 format manager 224 virus manager 226 security manager 230 Composition module

---

[Translation done.]

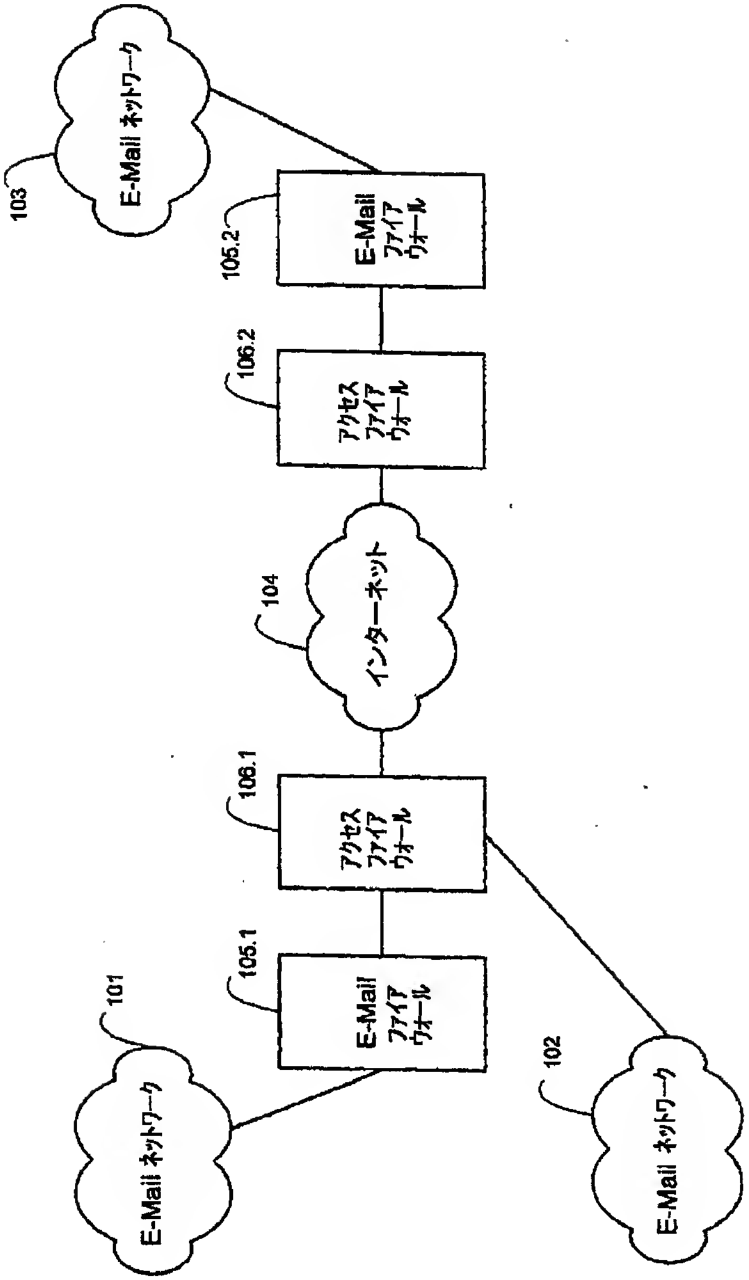
* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

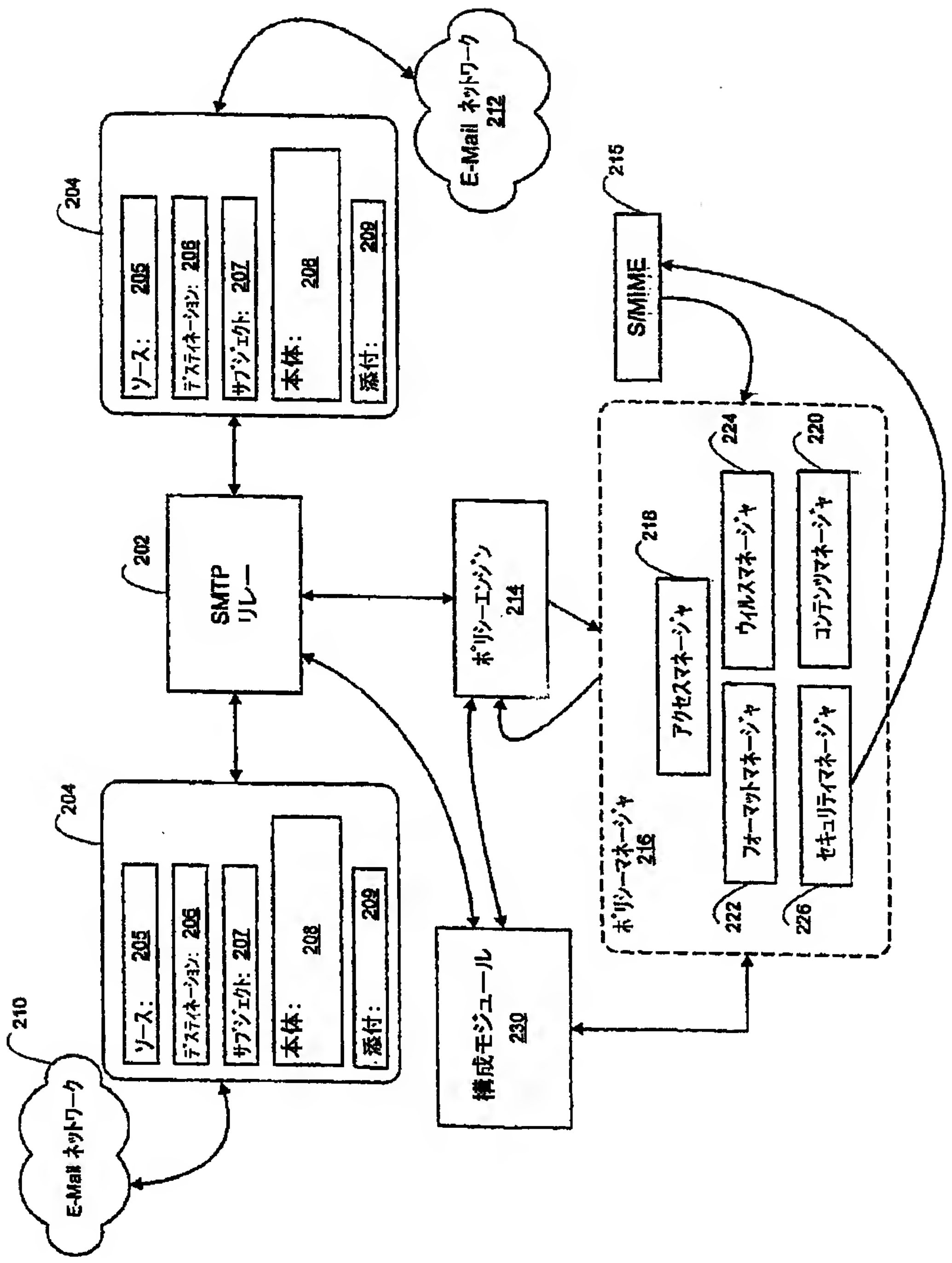
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

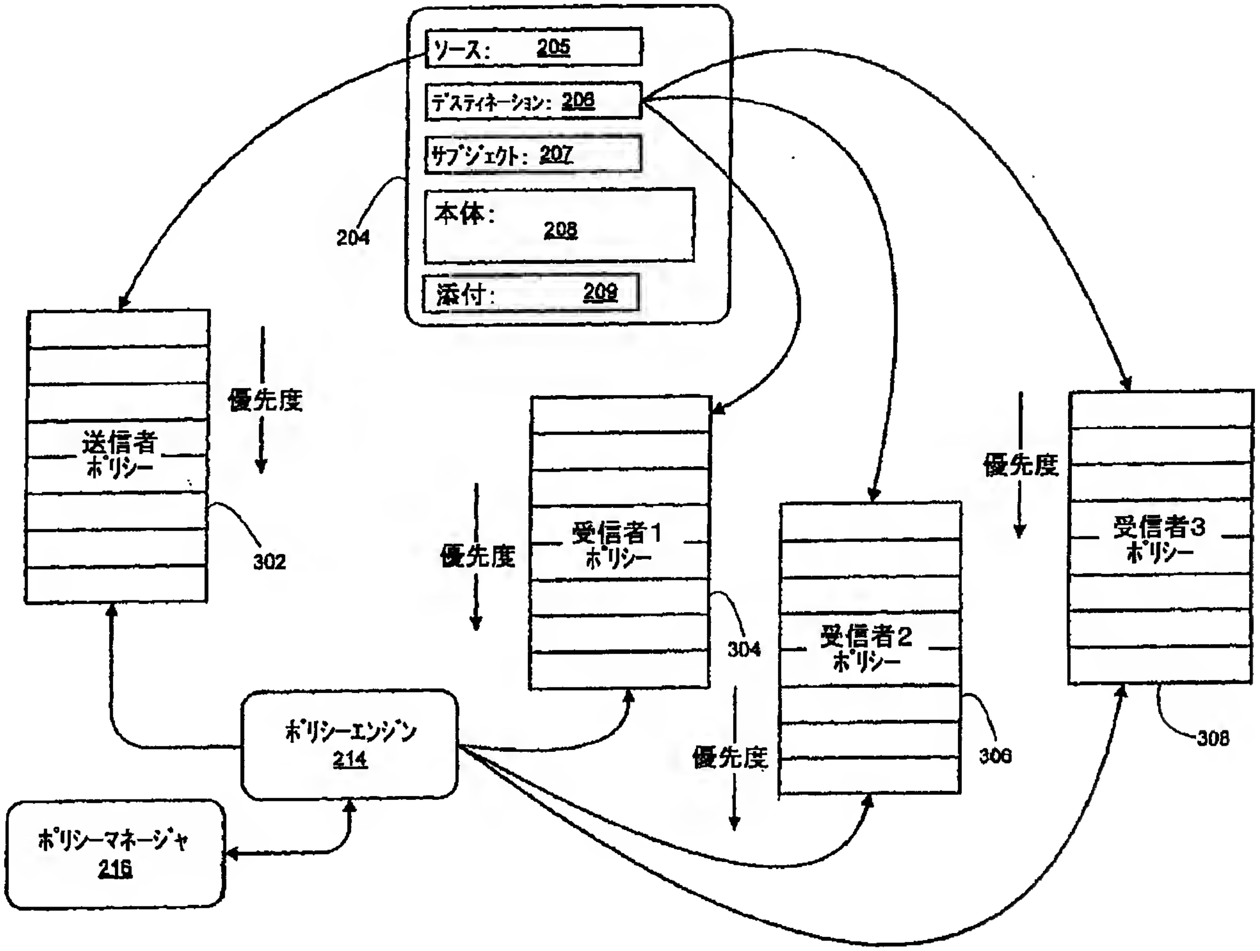
[Drawing 1]


103
E-Mail ネットワーク
105.2
E-Mail
ファイア
ウォール
106.2
アクセス
ファイア
ウォール
104
インターネット
106.1
アクセス
ファイア
ウォール
105.1
E-Mail
ファイア
ウォール
101
E-Mail ネットワーク
102
E-Mail ネットワーク

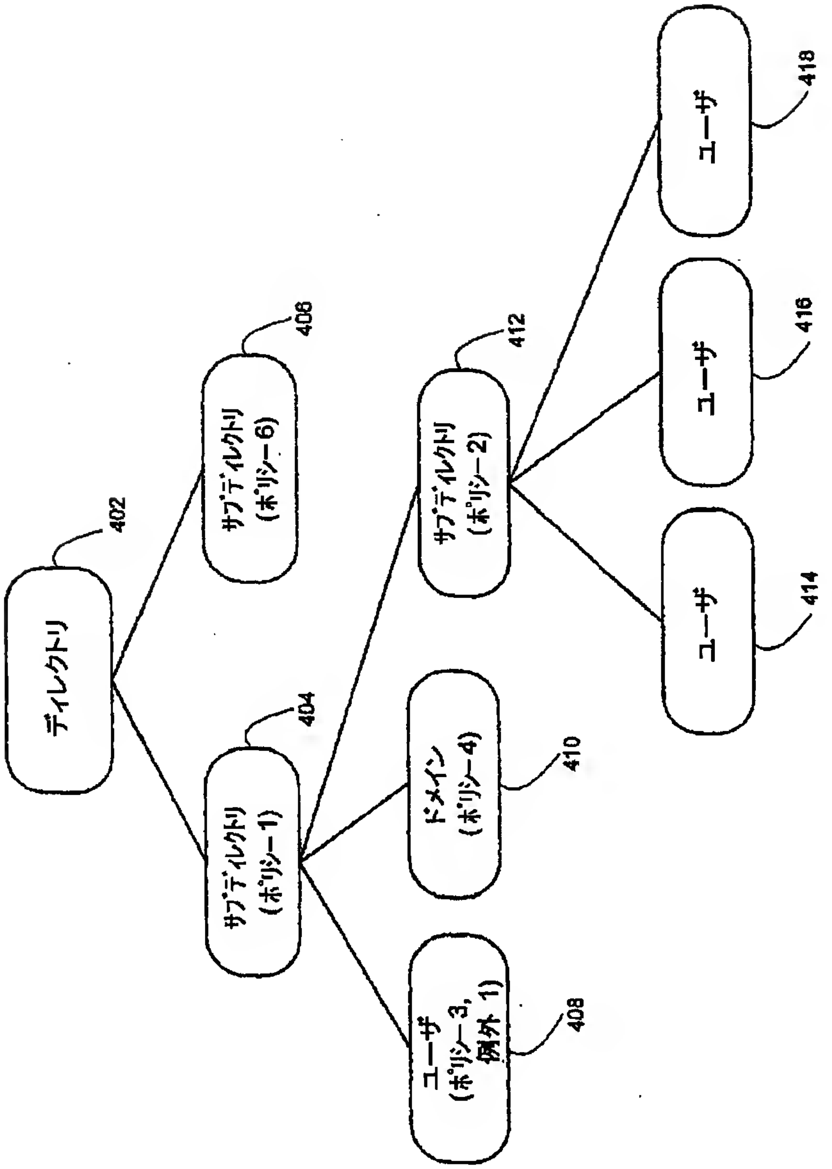
[Drawing 2]


204
ソース: 205
デスティネーション: 206
サブジェクト: 207
本体: 208
添付: 209
E-Mail ネットワーク 212
202
SMTP リレー
204
ソース: 205
デスティネーション: 206
サブジェクト: 207
本体: 208
添付: 209
210
E-Mail ネットワーク
ポリシーエンジン 214
構成モジュール 230
215
S/MIME
ポリシーマネージャ 216
218
アクセスマネージャ
224
ウィルスマネージャ
220
コンテンツマネージャ
222
フォーマットマネージャ
226
セキュリティマネージャ

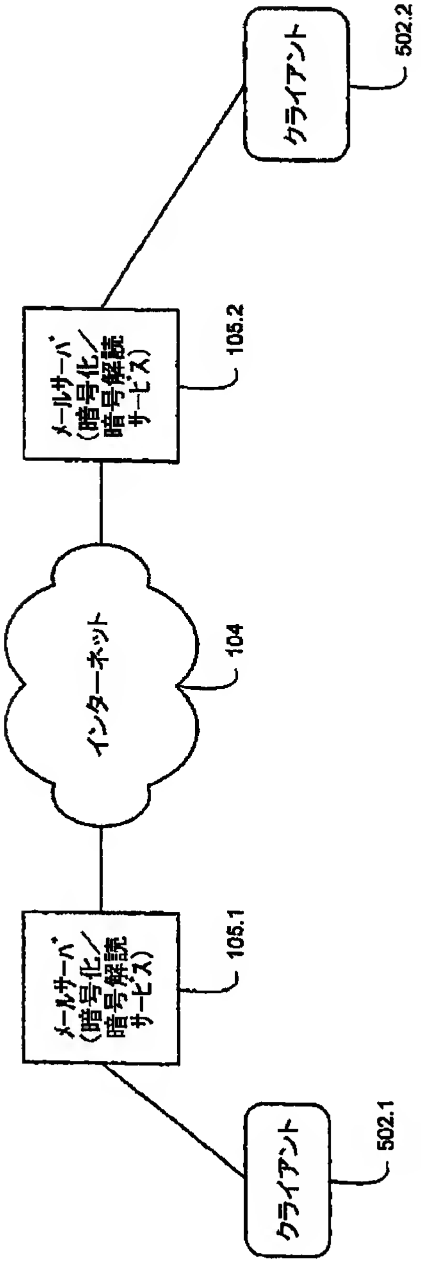
[Drawing 3]


ソース: 205
デスティネーション: 206
サブジェクト: 207
本体: 208
添付: 209
204
送信者ポリシー
302
優先度
受信者1ポリシー
304
優先度
受信者2ポリシー
306
優先度
受信者3ポリシー
308
優先度
ポリシーエンジン 214
ポリシーマネージャ 216

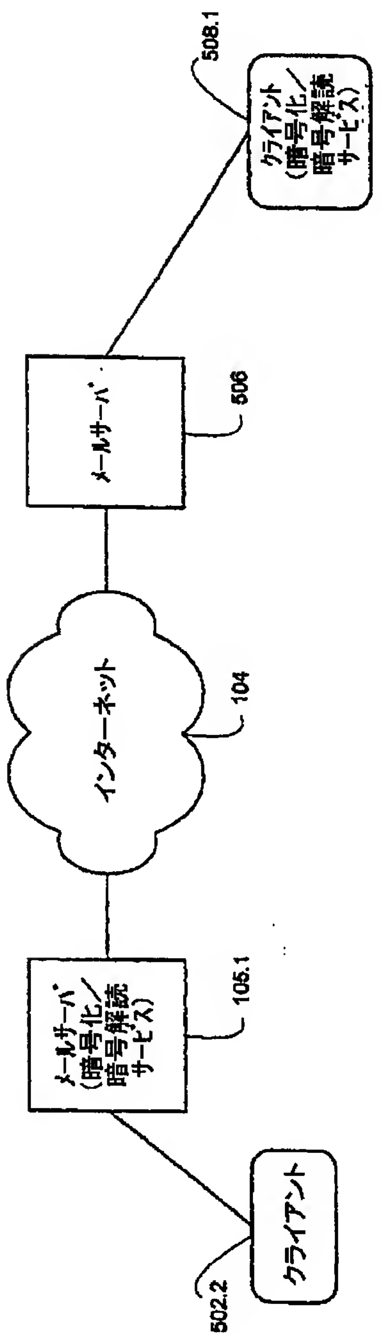
[Drawing 4]


ディレクトリ
402
サブディレクトリ（ポリシー6）
406
サブディレクトリ（ポリシー1）
404
ドメイン（ポリシー4）
410
ユーザ（ポリシー3, 例外1）
408
サブディレクトリ（ポリシー2）
412
ユーザ
414
ユーザ
416
ユーザ
418

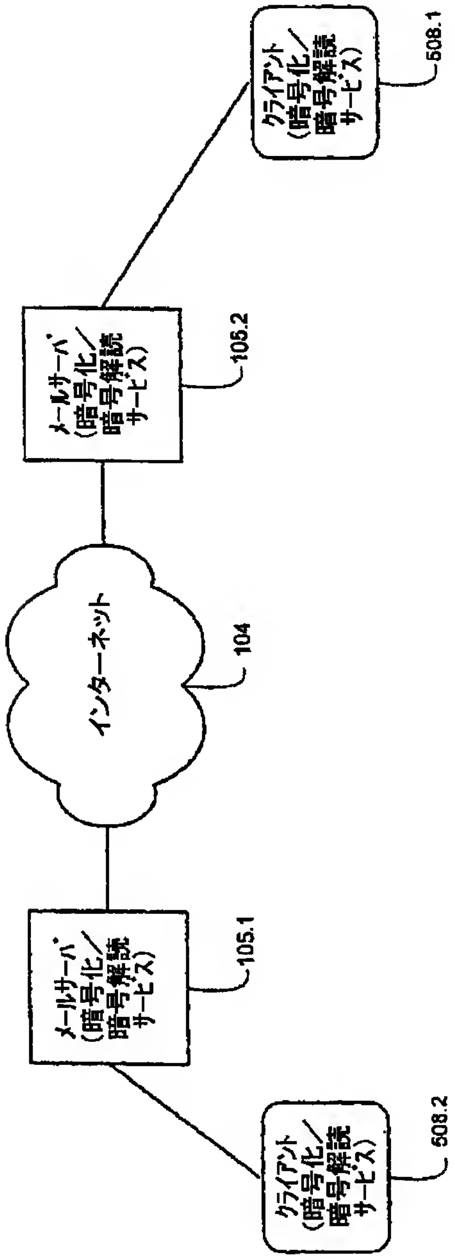
[Drawing 5 (a)]


クライアント
502.2
メールサーバ（暗号化／暗号解読サービス）
105.2
インターネット
104
メールサーバ（暗号化／暗号解読サービス）
105.1
クライアント
502.1

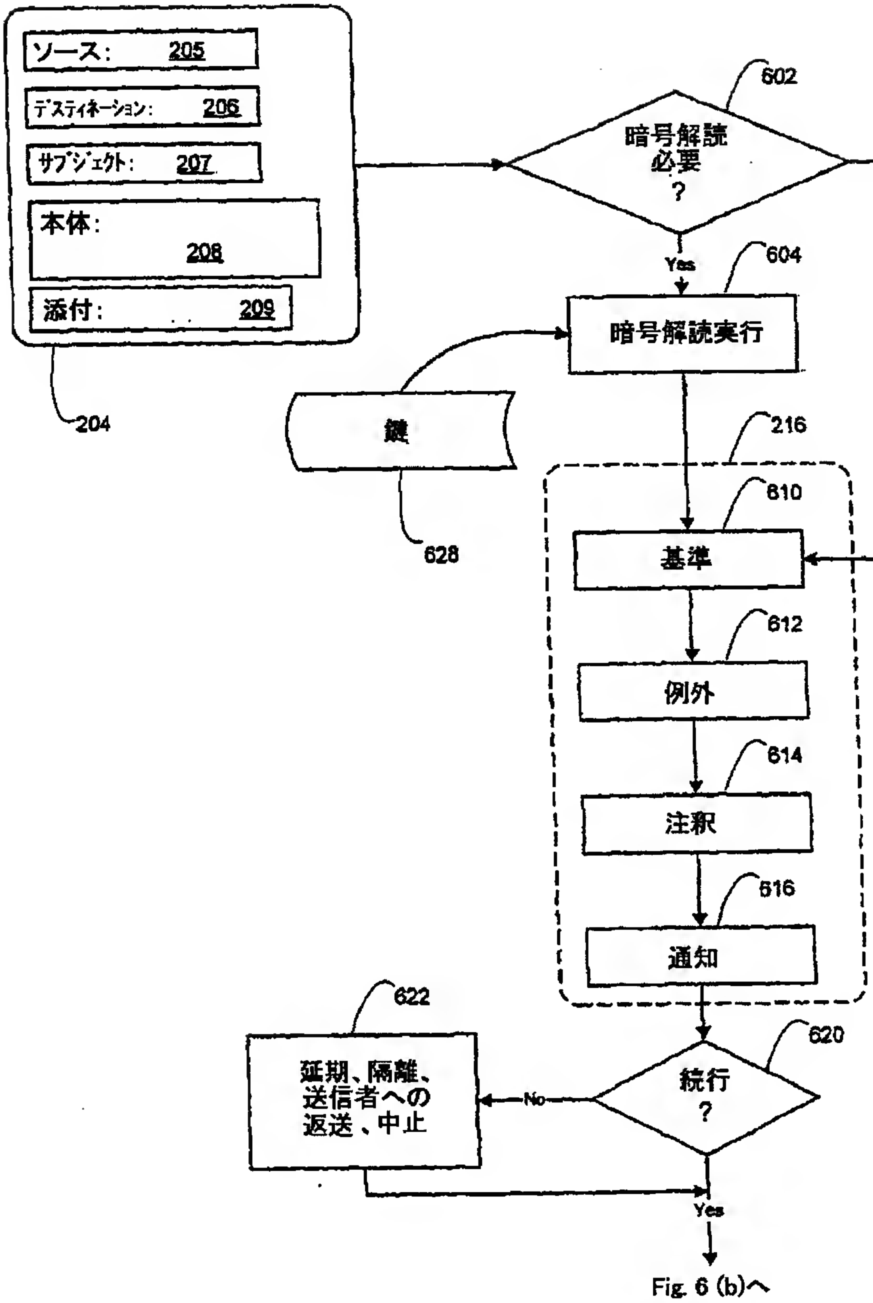
[Drawing 5 (b)]


クライアント
502.2
メールサーバ（暗号化／暗号解読サービス）
105.1
インターネット
104
メールサーバ
506
クライアント（暗号化／暗号解読サービス）
508.1

[Drawing 5 (c)]


クライアント（暗号化／暗号解読サービス）
508.2
メールサーバ（暗号化／暗号解読サービス）
105.1
インターネット
104
メールサーバ（暗号化／暗号解読サービス）
105.2
クライアント（暗号化／暗号解読サービス）
508.1

[Drawing 6 (a)]


ソース: 205
デスティネーション: 206
サブジェクト: 207
本体: 208
添付: 209
204
602
暗号解読必要？
Yes
No
604
暗号解読実行
鍵
628
216
610
基準
612
例外
614
注釈
616
通知
620
続行？
No
622
延期、隔離、送信者への返送、中止
Yes
Fig. 6 (b)へ

[Drawing 6 (b)]

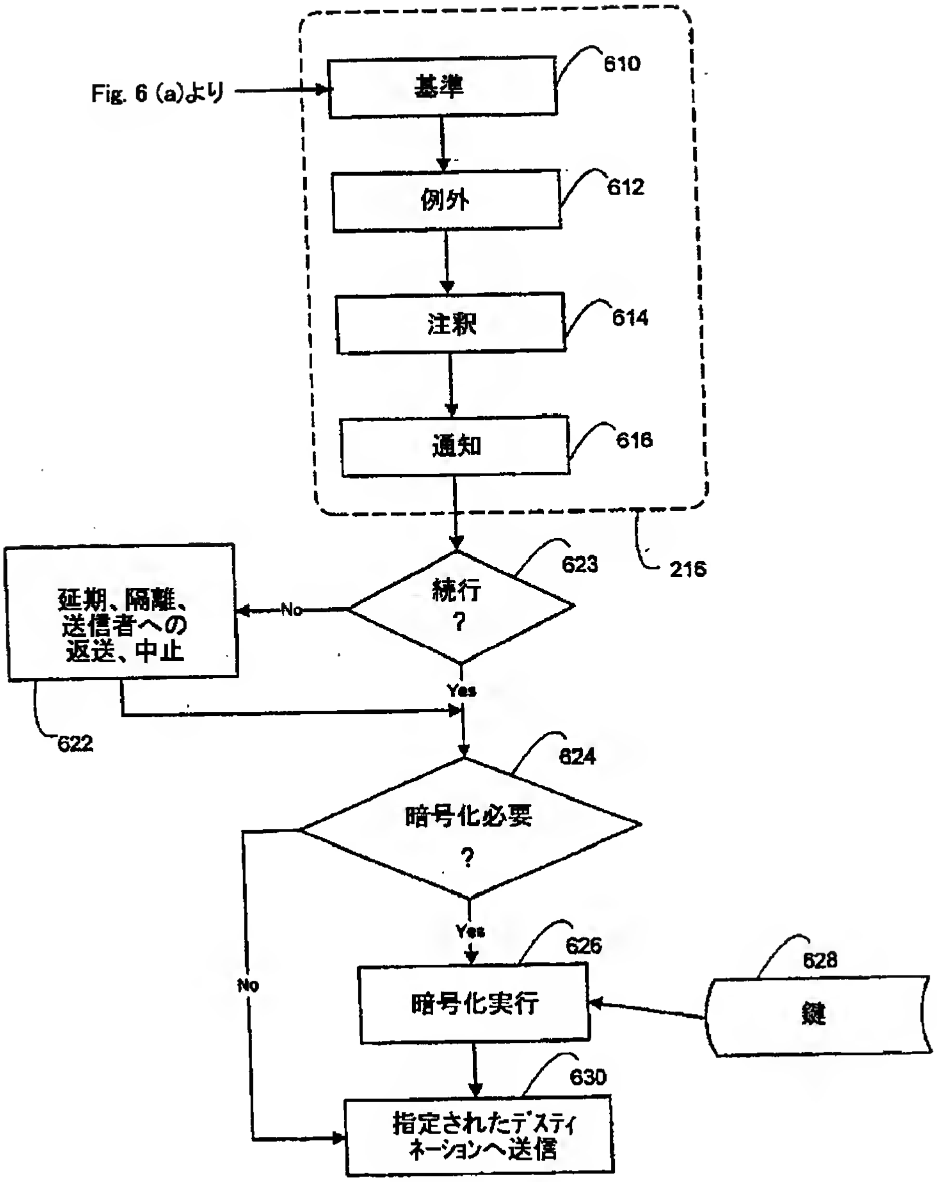
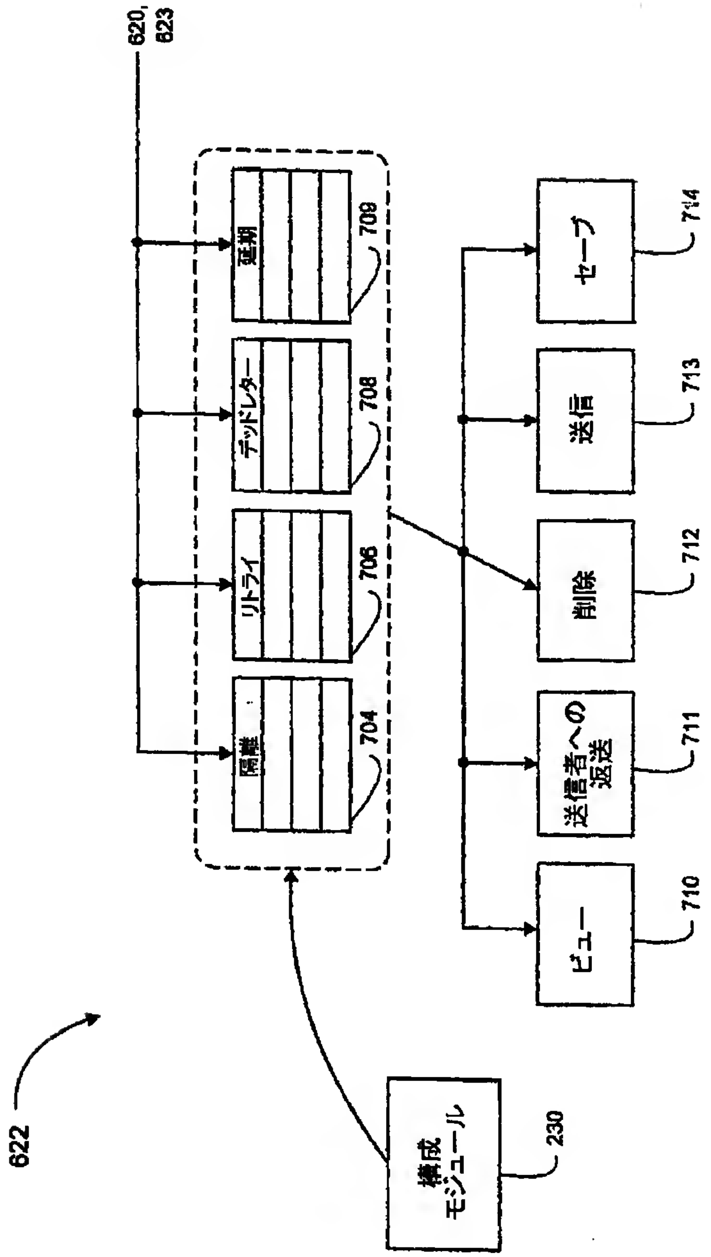


Fig. 6 (a)より
基準
610
例外
612
注釈
614
通知
616
216
続行
?
623
No
延期、隔離、送信者への返送、中止
622
Yes
暗号化必要
?
624
Yes
No
暗号化実行
626
鍵
628
指定されたデスティネーションへ送信
630

[Drawing 7]


622
620,
623
延期
709
デッドレター
708
リトライ
706
隔離
704
セーブ
714
送信
713
削除
712
送信者への返送
711
ビュー
710
構成モジュール
230

[Translation done.]